DRAWING AMENDMENTS

The Applicant respectfully requests approval of the amendment to Figure 2 as depicted in the Appendix accompanying this paper. The Appendix includes both a red line version of Figure 2, which is labeled "Annotated Sheet Showing Changes," as well as a new sheet that is labeled "Replacement Sheet" and which includes the amended Figure 2.

The proposed change adds reference a reference letter "M" that is described in the specification but that was inadvertently omitted from the drawings as originally filed, as noted in the objection to Figure 2 in the Office Action. The addition of the reference letter "M" is fully supported by the specification as filed, and no new matter is introduced.

Specifically, in Figure 2, the label for element 206 is changed from "MESSAGE INPUT" to "M MESSAGE INPUT" to correspond to the description of element 206 in the application on page 19, lines 3-5.

REMARKS

The Examiner is thanked for the performance of a thorough search.

SPECIFICATION

In the specification, new paragraph [90.1] has been added to describe element 420 of Figure 4, which was inadvertently omitted in the application as filed, as noted in the objection to Figure 4 in the Office Action.

The material in new paragraph [90.1] is fully supported by the application as filed. For example, new paragraph [90.1] is supported by at least the content of box 420 of Figure 420, as well as the application on page 6, paragraph [15] on lines 9-12, page 13, paragraphs [43] and [44] on lines 11-19, and page 15, paragraph [50] on lines 9-11. Therefore, no new matter is introduced.

DRAWINGS

In amended Figure 2, the label for element 206 is changed to read "M MESSAGE INPUT" to correspond to the description of element 206 in the application on page 19, lines 3-5, as required by the objection to Figure 2 in the Office Action. As such, no new matter is included because the change to Figure 2 is fully supported by the application as filed.

As noted above, the specification has been amended to refer to reference number 420 and the contents of box 420 as shown in Figure 4. As a result, the Applicant respectfully submits that the change to the specification traverses the objection to Figure 4 in the Office Action.

STATUS OF CLAIMS

Claims 1-6, 8-9, and 12 have been amended.

Claims 14-16 have been added.

No claims have been cancelled or withdrawn.

Claims 1-16 are currently pending in the application.

SUMMARY OF THE OBJECTIONS AND REJECTIONS

Figure 2 is objected to because Figure 2 lacks an input register M as described in the specification. Figure 4 is objected to because Figure 4 includes a reference character not described in the specification. The objections to the drawings are addressed above in the discussion of the amendments to the drawings and specification.

Claims 8-11 are objected to under 37 CFR 1.75(c) for allegedly being of improper dependent form. Claim 1 is rejected under 35 U.S.C. § 112, second paragraph, as allegedly incomplete. Claims 1-4, 6, 8, 9, and 12 are rejected under 35 U.S.C. § 112, second paragraph, as allegedly indefinite.

Claim 2 is rejected under 35 U.S.C. § 101 because the claimed invention is allegedly directed to non-statutory subject matter. Claims 1-13 are rejected under 35 U.S.C. § 101 because the claimed invention allegedly lacks patentable utility.

Claims 5 and 7-11 have been rejected under 35 U.S.C. § 102(b) as allegedly anticipated by U.S. Patent Number 4,759,063 issued to Chaum (" *Chaum* "). Claims 1-4, 12, and 13 have been rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over *Chaum* in view of "Applied Cryptography," 2nd Ed., pages 248-249 by Schneier (" *Schneier* "). The rejections are respectfully traversed.

OBJECTION TO CLAIMS 8-11 UNDER 37 CFR 1.75(c)

Claims 8-11 are objected to under 37 CFR 1.75(c) as allegedly being of improper dependent form for failing to further limit the subject matter of a previous claim. Specifically, the Office Action states that Claims 8-11 "modify the preamble of Claim 5 and as such do not further limit the body of the claim."

Claims 8-11 specify four different types of a "particular operation" that is referred to in the preamble of Claim 5, namely "a Rivest, Shamir, and Adleman encrypting operation" (Claim 8), "a Rivest, Shamir, and Adleman decrypting operation" (Claim 9), "a digital signature algorithm signing operation" (Claim 10), and "a digital signature algorithm verifying operation" (Claim 11). Claim 5 includes a preamble that states "An apparatus for performing a particular operation for using digital signatures on a network..."

Claim 5 has been amended above to include in the body of Claim 5 the "particular operation" that is referred to in the preamble of Claim 5. As a result, Claims 8-11 now modify a feature of the body of Claim 5, and therefore the Applicant respectfully submits that Claims 8-11 are of proper dependent form and that the objections to Claim 8-11 is thereby traversed.

REJECTION OF CLAIM 1 UNDER 35 U.S.C. § 112, 2nd PARAGRAPH

Claim 1 is rejected under 35 U.S.C. §112, 2nd paragraph, as allegedly being incomplete. Specifically, the Office Action states that Claim 1 is "incomplete for omitting essential steps, such omission amounting to a gap between the steps. See MPEP § 2172.01. The omitted steps are: There is no step for the generation of the digital signature."

It appears to the Applicant that this rejection of Claim 1 is based on the preamble of Claim 1 reading "A data processing method for generating a digital signature," whereas the last step of Claim 1 is "storing the multiplicative inverse in a computer hardware storage element for use in determining the digital signature of the electronic message." Thus, it appears that the Office Action has rejected Claim 1 because the preamble refers to "generating a digital signature" while Claim 1 does not include such a "generating a digital signature step."

Claim 1 is amended above so that the preamble reads "A data processing method for generating a multiplicative inverse for use in determining a digital signature..." As a result of the amendment to Claim 1, the preamble of Claim 1 matches the last step of Claim 1 and there is no "gap between the steps" as indicated in the Office Action. Therefore, the Applicant respectfully submits that the amendment to Claim 1 traverses the rejection of Claim 1 as being incomplete.

In addition, the Applicant notes that MPEP §2172.01 states that a rejection under 35 U.S.C. §112, 2nd paragraph is proper when a claim "fails to interrelate **essential** elements of the invention **as defined *by applicant(s)* in the specification**...." (Emphasis added.) MPEP §706.03(d), form paragraph 7.34.12, explains that in making a rejection under 35 U.S.C. §112, 2nd paragraph for "Essential Steps Omitted," that the Office Action provide "the rationale for considering the omitted steps critical or essential."

Nowhere in the Office Action is a rational provided for considering the step of "generation of the digital signature" critical or essential, nor is there anywhere in the specification in which the Applicant has described the generation of a digital signature as being critical or essential to the claimed invention. In fact, while the Applicant in the specification describes the novel use of using a modulo exponentiation block for a prime modulus for computing a multiplicative inverse as part of a digital signature algorithm, the specification and claims make clear that the invention is not just for use in generating a digital signature.

For example, the specification describes that obtaining a multiplicative inverse is useful with both the Rivest, Shamir, and Adleman public key algorithm and the digital signature algorithm (DSA). (Application, page 3, paragraphs [7] through [9].) Also, while the Application explains that the use of a modulo multiplicative inverse apparatus is illustrated by an electronic circuit that is fabricated for generating a digital signature according to DSA for use in digital signature implementations, the Application states that "embodiments of the invention are not limited to this context, but may be employed in other contexts as well," such as verifying DSA signatures or other signature protocols or in the Rivest, Shamir, and Adleman public key algorithm. (Application, page 10, paragraph [34].)

As yet another example, Claims 8-11 describe four different operations in which the approach for generating a multiplicative inverse based on a prime modulus and a modulo exponentiation block may be used, such as (1) a Rivest, Shamir, and Adleman encrypting operation, (2) a Rivest, Shamir, and Adleman decrypting operation, (3) a digital signature algorithm signing operation, and (4) a digital signature algorithm verifying operation. Only in the third of these four examples of using a multiplicative inverse with a prime modulus and a modulo exponentiation block is a digital signature generated, while in the verification of a digital signature, the signature already exists and is not generated while in Rivest, Shamir, and Adleman public key encryption or decryption, there is no signature at all.

Therefore, the Applicant respectfully submits that contrary to the implied assertion of the Office Action in rejecting Claim 1 under 35 U.S.C. §112, 2nd paragraph that "generation of the digital signature" is critical or essential, the Application's specification and claims are unambiguously clear that "generation of the digital signature" is not critical or essential to the apparatus for determining a modulo multiplicative inverse, as demonstrated by the examples cited above.

REJECTION OF CLAIMS 1-4, 12, AND 13 UNDER 35 U.S.C. § 112, 2^{ND} PARAGRAPH

Claims 1-4 and 12 have been rejected under 35 U.S.C. § 112, second paragraph, as allegedly indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Specifically, the Office Action states that the term "substantially ιquals" is a relative term which renders the claims indefinite. Claims 1-4 and 12 have been amended to remove the word "substantially." Therefore, the Applicant respectfully submits that the amendments to Claims 1-4 and 12 traverse the rejection.

Claim 6 has been rejected under 35 U.S.C. § 112, second paragraph, as allegedly indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Specifically, the Office Action states that Claim 6 describes the invention in the negative by pointing out what the invention is not. As originally written, Claim 6 recited "further comprising" before listing the two features that are not included in the apparatus of Claim 5. Claim 6 is amended above to remove the language "further comprising" and replace that phrase with "wherein the apparatus has" followed by the two features not included in the apparatus of Claim 5.

As explained in MPEP §2173.05(i), some "older cases were critical of negative limitations because they tended to define the invention in terms of what it was not, rather than pointing out the invention." However, MPEP §2173.05(i) also explains that the "current view of the courts is that ***there is nothing inherently ambiguous or uncertain about a negative limitation***. So long as the boundaries of the patent protection sought are set forth definitely, albeit negatively, the claim complies with the requirements of 35 U.S.C. 112, second paragraph." (Emphasis added.) As a result, the Applicant respectfully submits that Claim 6 is not indefinite and fully complies with 35 U.S.C. § 112, second paragraph.

Claims 8 and 9 have been rejected under 35 U.S.C. § 112, second paragraph, as allegedly indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Specifically, the Office Action states that Claims 8 and 9 "contain the trademark/trade name RSA." Claims 8 and 9 are amended above to remove the alleged trademark/trade name "RSA" and replace it with the "Rivest, Shamir, and Adleman" to denote the public key algorithm developed by Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman, features of which are described in U.S. Patent No. 4,405,829 that is listed on the Notice of References Cited Form PTO-892 accompanying the Office Action. This algorithm is commonly referred to as the Rivest, Shamir, and Adleman public key algorithm that is used for encryption and decryption and that is frequently abbreviated to RSA based on the their last names of the three individuals who developed the algorithm. A search of the trademark database at the U.S. Patent and Trademark Office's website fails to show any trademarks or trade names for "Rivest, Shamir, and Adleman." Therefore, the Applicant respectfully submits that the amendments to Claims 8 and 9 traverse the rejection.

REJECTION OF CLAIM 2 UNDER 35 U.S.C. § 101

Claim 2 is rejected under 35 U.S.C. § 101 because the claimed invention is allegedly directed to non-statutory subject matter. Specifically, the Office Action states that the method steps of Claim 2 manipulate abstract data and that there is no "useful, concrete, and tangible" result.

Claim 2 is amended above to include the following feature: "wherein the output generated by the modulo exponentiation block is stored in a computer hardware storage element for use in performing a particular operation that is selected from the group consisting of a digital signature algorithm signing operation, a digital signature algorithm verifying operation, an encryption operation for a first electronic message, and a decryption operation for a second electronic message."

As amended above, Claim 2 includes a similar computer hardware storage element feature as in Claim 1, and Claim 2 includes four different types of uses for the output of the modulo exponentiation block, such as those in Claims 8-11. Each of the four uses in Claim 2 reflects a result that is useful, concrete, and tangible since the output of the modulo exponentiation block is used in signing with a digital signature, verifying a digital signature, encrypting an electronic message, or decrypting an electronic message.

Therefore, the Applicant respectfully submits that Claim 2, as amended above, traverses the rejection of Claim 2 under 35 U.S.C. § 101.

REJECTION OF CLAIMS 1-13 UNDER 35 U.S.C. § 101

Claims 1-13 are rejected under 35 U.S.C. § 101 because the claimed invention allegedly lacks patentable utility. Specifically, the Office Action states that Claims 1-13 "manipulate[] abstract data to an intermediate step, but does not actually produce the digital signature or any other tangle result."

The Applicant respectfully disagrees that Claims 1-13 lack patentable utility. For example, in Claim 1, the result is the "storing of the multiplicative inverse in a computer hardware storage element for use in determining the digital signature of the electronic message." As a result of the approach of Claim 1, the multiplicative inverse that is needed for implementing the Rivest, Shamir, and Adleman public key algorithm and the digital signature algorithm (DSA) is obtained via modular exponentiation instead of through the use of the extended Euclidean algorithm (EEA) without special purpose hardware, as in conventional systems as described in the specification. (Application, page 3, paragraph [8] – page 4, paragraph [9].) Thus, the approach of Claim 1 represents an improvement over conventional approaches, thereby providing a utility that is patentable. Similarly, Claims 2-13 involve the use of a modulo exponentiation block or function that can be similarly used in various applications, such as encryption/decryption with the Rivest, Shamir, and Adleman public key algorithm or signature signing or verifying with DSA.

Furthermore, based on the Office Action not including Claims 1 and 3-13 along with Claim 2 in the previous rejection under 35 U.S.C. § 101 based on the alleged lack of a "useful, concrete, and tangible" result, the Office Action has recognized that Claims 1 and 3-13 have a "useful, concrete, and tangible" result, which is contrary to the assertion of the Office Action in the second 101 rejection that Claims 1-13 lack patentable utility due to allegedly failing to "actually produce the digital signature or any other tangible result."

In addition, the Applicant respectfully disagrees with the position of the Office Action that Claims 1-13 must actually produce a digital signature or any other particular utility, since the novel approach for determining the multiplicative inverse through modular exponentiation can be used in any of a number of applications, such as encryption/decryption with the Rivest, Shamir, and Adleman public key algorithm or signature signing or verifying with DSA. (Application, page 10, paragraph [34].)

Also, the Applicant respectfully disagrees with the position of the Office Action that Claims 1-13 merely manipulate abstract data. Each of Claims 1-13 features more than abstract data, namely the determination of a multiplicative inverse that represents a useful quantity by itself, such as indicated in the different example uses and implementations described in the application, such as digital signature signing and verification, as in DSA, and encryption and decryption of electronic messages, as with the Rivest, Shamir, and Adleman public key algorithm.

Furthermore, according to MPEP §2107, if during examination "it becomes readily apparent that the claimed invention has a well-established utility, do not impose a rejection based on lack of utility. An invention has a well-established utility if (i) a person of ordinary skill in the art would immediately appreciate why the invention is useful based on the characteristics of the invention (e.g., properties or applications of a product or process), and (ii)the utility is specific, substantial, and credible." The Office Action itself evidences that Claims 1-13 include "a well-established utility" when the Office Action states one of the particular applications described in the application, namely producing a digital signature.

Also, MPEP §2107 states: "If the applicant has asserted that the claimed invention is useful for any particular practical purpose (i.e., it has a 'specific and substantial' utility') and the assertion would be considered credible by a person of ordinary skill in the art, do not impose a rejection based on lack of utility." Again, the Office Action's own recognition of the "specific and substantial utility" of producing a digital signature evidences that Claims 1-13 have patentable utility as asserted in the Application and that such an assertion is credible. Plus the Application itself describes that the claimed invention can be used in any of a number of embodiments requiring the calculation of a multiplicative inverse, including but not limited to, digital signature signing and verifying, such as with DSA, or electronic message encryption and decryption, such as with the use of the Rivest, Shamir, and Adleman public key algorithm. (Application, page 10, paragraph [34].)

In addition, MPEP §703.03(a)(II) states: "A rejection on the ground of lack of utility includes the more specific grounds of inoperativeness, involving perpetual motion, frivolous, fraudulent, and against public policy." Within MPEP §703.03(a)(II), form paragraph 7.05.02 for "Utility Lacking" states that the Office Action "provide explanation of lack of utility, such as, for example, that which is frivolous, fraudulent, against public policy." Yet the Office Action fails to provide any explanation as to why the claimed invention involves perpetual motion, is frivolous, is fraudulent, or is against public policy."

In light of the specific and substantial utility recognized in the Office Action's rejection itself, namely the production of a digital signature, in addition to the other specific and substantial utilities described in the application, namely digital signature signing and verifying and encryption and decryption of electronic messages (e.g., Application, page 10, paragraph [34], et. seq.), the Applicant respectfully submits that Claims 1-13 include patentable utility and respectfully request that the rejection of Claims 1-13 under 35 U.S.C. § 101 be withdrawn.

RESPONSE TO REJECTIONS BASED ON THE PRIOR ART

To summarize the following discussion, the approaches of the claims of the present application involve the use of modulo exponentiation block or function to determine a multiplicative inverse based on using a prime modulus. As a result, the approaches of the claims can be implemented without the conventional extended Euclidean algorithm (EEA), which is an iterative algorithm for computing a multiplicative inverse, and which involves a modular inverter circuit for determining the multiplicative inverse. The cited prior art of *Chaum* and *Schneier* are merely examples of implementations that use the iterative EEA conventional approach and both cited prior art references lack any teaching, suggestion, or disclosure of the use of a modulo exponentiation block or function to determine a multiplicative inverse based on using a prime modulus.

A. CLAIM 1

(1) INTRODUCTION TO CLAIM 1

Claim 1 features:

> "A data processing method for generating a multiplicative inverse for use in determining a digital signature, the method comprising the computer-implemented steps of:
>
> receiving and storing a first integer data value relating to a digital signature of an electronic message;
>
> determining a multiplicative inverse of the first integer data value modulo a prime modulus data value by **computing a *first quantity* modulo the prime modulus data value**, wherein said computing includes using a ***modulo exponentiation block***;
>
> wherein the ***first quantity*** **equals, modulo the prime modulus data value, the first integer data value raised to a power of a *second quantity***;
>
> wherein the ***second quantity*** **is two less than the prime modulus data value**; and

storing the multiplicative inverse in a computer hardware storage element for use in determining the digital signature of the electronic message." (Emphasis added.)

As an example of the approach of Claim 1, the features of Claim 1 correspond to an implementation of expression (23) in the application, namely $a^{p-2} = a^{-1}$ mod p, in which a modulo multiplicative inverse, a^{-1} mod p, is determined based on modulo exponentiation, a^{p-2} mod p, for p being a prime modulus. The approach of Claim 1 is implemented using a modulo exponentiation block, which avoids the problems of using the extended Euclidean algorithm (EEA) that is an iterative approach and slow for large numbers, which is today common with key sizes of 1024, 2048, or even more bits. As explained in the Application, EEA is typically implemented as a multiplicative inverse (MI) block through an application specific integrated circuits (ASICs), that occupy a large area of chip "real estate." (Application, pages 3-4.)

However, in the approach of Claim 1, existing blocks, such as a modulo exponentiation (ME) block, can be used that have smaller area requirements when implemented on a chip. This improvement is at the "expense" of requiring that the modulus be a prime modulus, which is required in deriving expression (23) as illustrated in the Application, although such an expense is generally outweighed by the result of being able to calculate a multiplicative inverse using modular exponentiation in lieu of an ASIC that implements the larger and more time consuming MI circuitry.

Specifically in Claim 1, the modulo exponentiator block is used in "determining a multiplicative inverse of the first integer data value modulo a prime modulus by computing a first quantity modulo the prime modulus data value." For example, the first integer data value is the value for which the multiplicative inverse is desired, such as "a" in expression (23) of the application. The prime modulus is "p" in expression (23).

Next in Claim 1, the "first quantity equals, modulo the prime modulus data value, the first integer data value raised to a power of a second quantity." For example, the first quantity is "a" in expression (23) modulo the prime modulus "p" raised to the power of the second quantity.

Then in Claim 1, the "second quantity is two less than the prime modulus data value." For example, the second quantity is the exponent of expression (23), namely "p-2" or two less than the prime modulus.

Note that while this example of the approach of Claim 1 is described in the context of the embodiment of the Application as represented by expression (23), Claim 1 is not limited to embodiments that correspond to expression (23).

(2) INTRODUCTORY DISCUSSION OF *CHAUM* AND *SCHNEIER*

In contrast to the approach of Claim 1, *Chaum* discloses "blind signature systems" in which messages are transformed in such a way that the signer of the messages cannot determine which transformed message corresponds with which digital signature. (Abstract.) For example, in the electronic banking context, the blind signature approach of *Chaum* avoids the problem of payment systems in which a bank is always able to know which account a note was withdrawn from and which account it was deposited to, thereby presenting problems of personal privacy to the sender and recipient of the note. (Col. 2, lines 45-49.) Also in contrast to the approach of Claim 1, *Schneier* discloses approaches for calculating inverses, such as Euler's generalization and Euclid's algorithm, both of which define expressions for the inverse "x" in terms of the inverse itself. Thus, both formulations for determining multiplicative inverses in *Schneier* are iterative approaches.

In the detailed description, *Chaum* describes the used of a "modular multiplicative inverter" as illustrated in Figure 3 and described in the specification in Columns 13 and 14. Note that as illustrated in Figure 3, *Chaum's* modular multiplicative inverter does not include a modulo exponentiation block, but merely a modulo multiplier (element 304) and a modular subtractor (element 305). *Chaum* describes the details of the modular inverter of Figure 3 by explaining that input from line 351 is taken and produces an output that is congruent to the multiplicative inverse of the input based on a variation of Euclid's algorithm. (Col. 13, line 62 – Col. 14, line 1.) *Chaum* then presents a table that illustrates the iterative operation of the modular inverter that clearly shows the iterative nature of *Chaum's* modular inverter based on the six iterations provided in the table that are required to reach the final desired result.

Thus, the modular inverter of *Chaum* is nothing more than the iterative EEA method described as the conventional approach of the Applicant's specification, which is also represented as Euclid's algorithm in *Schneier*. However, neither *Chaum* nor *Schneier* disclose the use of a modulo exponentiator block or function with a prime modulus for calculating a multiplicative inverse, as in the approach of Claim 1.

(3) THE OFFICE ACTION'S CITATIONS FROM *CHAUM* AND *SCHNEIER*

In the rejections of the claims over the prior art under either 102(b) or 103(a), the Office Action fails to even allege that either *Chaum* or *Schneier* disclose a modulo exponentiator block as featured in Claims 1-15. Instead, the Office Action states in the rejection of Claim 5 that "Chaum teaches a modular multiplicative inverter (column 13, lines 33-35 and Figure 3)," and then the Office Action states in the rejection of Claims 1-4 and 12, that "Chaum teaches...Computing a multiplicative inverse using modular arithmetic (column 13, lines 33-67)." Thus, it appears to the Applicant that the Office Action's rejections based on the prior art of based on equating the modular multiplicative inverter described in Column 13 of *Chaum* and illustrated in Figure 3 as being the same as the modulo exponentiation block or function of Claims 1-15.

However, as discussed above, the modular multiplicative inverter illustrated in Figure 3 of *Chaum* only includes a modular multiplier 304 and a modular subtractor 305, and there is nothing like a modular exponentiation block or function illustrated in Figure 3 nor described in the accompanying initial description of Figure 3 in the specification (e.g., Col. 13, lines 33-61), nor in the longer, more detailed description of the operation of the multiplicative inverter in the immediately following portion of the specification (e.g., Col. 13, line 62 – Col. 14, line 55.)

In fact, after a careful reading of the prior art references, the modular multiplicative inverter of Figure 3 of *Chaum* can be recognized as merely implementing the iterative extended Euclidean algorithm (EEA), as evidenced by the iterative example of the Table of Column 14 in *Chaum* that shows six iterations to obtain the desired result. This is consistent with the expression for the Euclidian algorithm on page 249 of *Schneier* in which the expression for the inverse is given in terms of the inverse itself, thus necessitating an iterative approach to obtain the desired inverse, as typified by the example in *Chaum*. As described above, the iterative approach for determining a modular multiplicative inverse based on

Euclid's algorithm, such as with the EEA, fails to involve the use of a modulo exponentiator block or function, as in the approach of Claim 1 or any of the other claims of the application.

As an additional observation, the Application notes that *Chaum* does show exponentiators 122 and 124 in Figure 1 and a modular exponentiator in Figure 4. However, none of these exponentiators is used to determine a multiplicative inverse based on a prime modulus as in Claim 1. Specifically, exponentiators 122 and 124 are illustrated for a blind signature system as performing conventional modular exponentiation as part of the digital signature algorithm while modular inverter 126 is a high level representation of the modular inverter of Figure 3 of *Chaum*. (Col. 11, line 41 – Col. 12, line 67.) Also, the modular exponentiator of Figure 4 merely performs conventional modular exponentiation as required by the blind digital signature approach and is not used for performing modular exponentiation as part of determining a multiplicative inverse based on modular exponentiation and a prime modulus.

(4) CONCLUSION OF DISCUSSION OF CLAIM 1 AND *CHAUM* AND *SCHNEIER*

Because *Chaum* and *Schneier*, either alone or in combination, fail to disclose, teach, suggest, or in any way render obvious "determining a multiplicative inverse...**using a *modulo exponentiation block*"** by "**computing a first quantity modulo the prime modulus data value**" in which "the ***first quantity*** **equals, modulo the prime modulus data value, the first integer data value raised to a power of a *second quantity*"** and "the ***second quantity*** **is two less than the prime modulus data value**," the Applicant respectfully submits that, for at least the reasons stated above, Claim 1 is allowable over the art of record and is in condition for allowance.

C. CLAIMS 2-5, 12, AND 14-16

Independent Claims 2-5, 12, and 14-16 contain features that are either the same as or similar to those described above with respect to Claim 1. For example, all of Claims 2-5 and 14-16 include the use of a "modulo exponentiation block" for determining "a multiplicative inverse" based on a "prime modulus," all of which is the same as in Claim 1. Similarly, Claim 12 includes the use of a "modulo exponentiation function," which is similar to Claim 1.

In addition, the modulo exponentiation block or function used for determining the multiplicative inverse in Claims 2-4, 12, and 14-16 is based on two quantities or values, in which the first quantity/value, modulo the prime modulus, equals the input/integer value raised to a second quantity/value that in turn is two less than the prime modulus, which is similar to Claim 1.

Therefore, based on at least the reasons stated above with respect to Claim 1, the Applicant respectfully submits that Claims 2-5, 12, and 14-16 are allowable over the art of record and are in condition for allowance.

In addition, Claim 5 features an apparatus "comprising a modulo exponentiator block configured for producing a multiplicative inverse of an integer modulo a prime modulus…" The Office Action rejected Claim 5 based only on *Chaum* citing Figure 3 and the associated description of Figure 3. Yet as explained above, neither Figure 3 of *Chaum* nor the associated description of Figure 3 illustrate or describe a modulo exponentiator block, little less a modulo exponentiator block that is "configured for producing a multiplicative inverse of an integer modulo a prime modulus…," as in Claim 5.

Thus, Claim 5 typifies the fundamental difference between the approaches of the claims of the present application and the prior art, since Claim 5 and the other claims involve computing a multiplicative inverse based on a prime modulus and modular exponentiation, whereas the prior art of *Chaum* and *Schneier* implements the iterative Euclidean-based approach for determining a multiplicative inverse that neither involves modular exponentiation, nor the use of a prime modulus.

D. CLAIMS 6-11 AND 13

Claims 6-11 and 13 are dependent upon Claims 5 and 12, respectively, and thus include each and every feature of the corresponding independent claims. Each of Claims 6-11 and 13 is therefore allowable for the reasons given above for Claims 5 and 12. In addition, each of Claims 6-11 and 13 introduces one or more additional limitations that independently render it patentable. However, due to the fundamental differences already identified, to expedite the positive resolution of this case a separate discussion of those limitations is not included at this time. Therefore, it is respectfully submitted that Claims 6-11 and 13 are allowable for the reasons given above with respect to Claims 5 and 12.

CONCLUSION

The Applicant believes that all issues raised in the Office Action have been addressed and that allowance of the pending claims is appropriate. After entry of the amendments, further examination on the merits is respectfully requested.

The Examiner is respectfully requested to contact the undersigned by telephone if it is believed that such contact would further the examination of the present application.

For the reasons set forth above, it is respectfully submitted that all of the pending claims are now in condition for allowance. Therefore, the issuance of a formal Notice of Allowance is believed next in order, and that action is most earnestly solicited.

To the extent necessary to make this reply timely filed, the Applicant petitions for an extension of time under 37 C.F.R. § 1.136.

If any applicable fee is missing or insufficient, throughout the pendency of this application, the Commissioner is hereby authorized to any applicable fees and to credit any overpayments to our Deposit Account No. 50-1302.

Respectfully submitted,
HICKMAN PALERMO TRUONG & BECKER LLP

Date: November 10, 2005

Craig G. Holmes
Reg. No. 44,770

2055 Gateway Place, Suite 550
San Jose, CA 95110-1089
Telephone: (408) 414-1207
Facsimile: (408) 414-1076

Appendix

CERTIFICATE OF MAILING
I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Hon. Commissioner for Patents, Mail Stop AMENDMENT, P.O. Box 1450, Alexandria, VA 22313-1450.

on Nov. 10, 2005 by Trudy Bagdon

APPENDIX

with

Annotated Sheet Showing Changes

and

Replacement Sheet

for Figure 2

ANNOTATED SHEET SHOWING CHANGES
Title: Method And Apparatus For Calculating A Multiplicative Inverse Of An Element Of A Prime Field
Inventor(s): Mahesh S. Maddury, et al.
Serial No. 10/040,050 Filing Date: October 25, 2001
Docket No: 50325-0598 Sheet 1 of 2

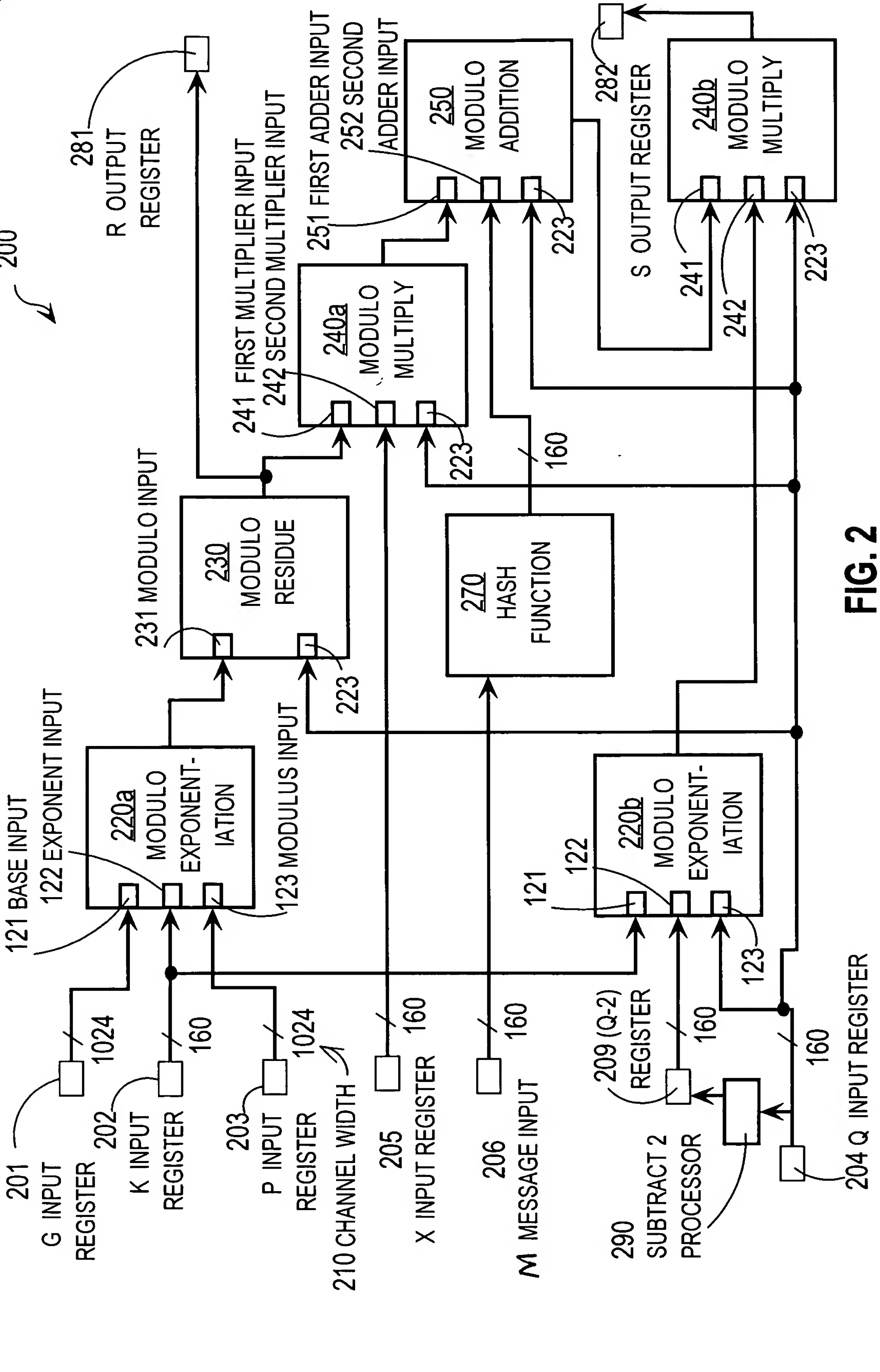

FIG. 2